(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 41 42 964 A 1**

(51) Int. Cl.[5]:
G 07 C 9/00
G 07 F 7/08

(21) Aktenzeichen: P 41 42 964.8
(22) Anmeldetag: 24. 12. 91
(43) Offenlegungstag: 1. 7. 93

DE 41 42 964 A 1

(71) Anmelder:
GAO Gesellschaft für Automation und Organisation mbH, 8000 München, DE

(74) Vertreter:
Klunker, H., Dipl.-Ing. Dr.rer.nat.; Schmitt-Nilson, G., Dipl.-Ing. Dr.-Ing.; Hirsch, P., Dipl.-Ing., Pat.-Anwälte, 8000 München

(72) Erfinder:
Pichlmaier, Albert; Meister, Gisela, Dr., 8000 München, DE

(54) Datenaustauschsystem mit Überprüfung der Vorrichtung auf Authentisierungsstatus

(57) Die Erfindung betrifft ein Datenaustauschsystem, bei dem die Berechtigung eines Benutzers durch die Überprüfung eines vom Benutzer eingegebenen persönlichen Merkmals festgestellt wird, mit einem dem Benutzer zugeordneten Datenträger, einer mit dem Datenträger kommunizierenden Vorrichtung und einer Anzeigeeinheit. Die Daten des Datenträgers enthalten ein nur dem Benutzer bekanntes Datenwort, das vor der Aufforderung zur Eingabe des persönlichen Merkmals zur Vorrichtung in codierter Form übertragen und nach der Decodierung durch eine in der Vorrichtung enthaltene und die Echtheit der Vorrichtung kennzeichnende kryptografische Einheit dem Benutzer zum Vergleich angezeigt wird.

DE 41 42 964 A 1

Beschreibung

Die Erfindung betrifft ein Datenaustauschsystem gemäß dem Oberbegriff des Anspruchs 1.

Aus der DE-PS 26 21 269 ist ein Datenaustauschsystem mit Datenträger und Vorrichtung bekannt, bei dem in dem Datenträger ein Datenspeicher vorgesehen ist. In diesem ist ein persönliches Merkmal, wie z. B. eine persönliche Idenfizierungsnummer (PIN) des rechtmäßigen Benutzers zu Vergleichszwecken gespeichert.

Bevor mit dem Datenträger eine Transaktion im Datenaustauschsystem vorgenommen werden kann, muß der Benutzer des Datenträgers über die Tastatur der Vorrichtung eine persönliche Identifizierungsnummer eingeben. Diese wird in den Datenträger übertragen und dort von einem Vergleicher auf ihre Identität mit der dem rechtmäßigen Benutzer zugeordneten Identifizierungsnummer geprüft. Im positiven Fall geht das Datenaustauschsystem davon aus, daß der rechtmäßige Besitzer des Datenträgers eine Transaktion vornehmen will und gibt eine Transaktionsfreigabe.

Wie vorstehend erläutert, spielt die PIN die wesentliche Rolle bei der Autorisierungsprüfung, denn jeder Dritte, der im Besitz des Datenträgers sowie der zugehörigen PIN ist, kann den Datenträger mißbräuchlich verwenden. Bei dem bekannten System wird die PIN eingegeben, ohne daß es dem Benutzer möglich ist, zu erkennen, ob er seinen Datenträger in eine manipulierte Vorrichtung eingibt und seine PIN mißbräuchlich verwendet wird.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, die Sicherheit des bekannten Datenaustauschsystems im Hinblick auf die Verarbeitung des persönlichen Merkmals zu verbessern.

Diese Aufgabe wird durch das im kennzeichnenden Teil des Anspruchs 1 angegebene Merkmal gelöst.

Das Wesentliche der Erfindung ist, daß dem Benutzer die Möglichkeit gegeben wird, vor der Preisgabe seines persönlichen Merkmals die Echtheit des Systems bzw. der Vorrichtung auf einfache Weise zu überprüfen.

In einer bevorzugten Ausführungsform der Erfindung ist das in dem Datenträger gespeicherte Datenwort ein einfach zu merkender Code, der nach einer Entschlüsselung durch eine echte Vorrichtung auf der Anzeige dieser Vorrichtung erscheint, wobei der Benutzer dann davon ausgehen kann, daß es sich um eine autorisierte Vorrichtung handelt. Denn nur diese ist in der Lage, das Codewort zu entschlüsseln, da nur eine autorisierte Vorrichtung über die notwendigen Entschlüsselungseinrichtungen verfügt.

In einer weiteren bevorzugten Ausführungsform ist vorgesehen, daß der Benutzer das Datenwort bestimmen und gegebenenfalls jederzeit, vorzugsweise nach korrekter PIN-Eingabe ändern kann.

In einer weiteren bevorzugten Ausführungsform wird die Überprüfung der Echtheit des Systems durch den Benutzer eingebunden in das in den meisten Fällen ohnehin notwendige Authentisierungsverfahren der Systemkomponenten. Eine Authentisierung der Systemkomponenten, Datenträger und Vorrichtung läuft im allgemeinen so ab, daß verschlüsselte Nachrichten zwischen den Komponenten ausgetauscht werden und in der jeweils anderen Systemkomponente zur Überprüfung der Echtheit der jeweils anderen Komponente verifiziert werden.

In einer weiteren bevorzugten Ausführungsform wird das Datenwort in die vom Datenträger zur Vorrichtung zu übertragende Nachricht eingebunden.

In einer anderen bevorzugten Ausführungsform wird ein Datenträger mit IC verwendet, das einen Speicher und eine Steuereinrichtung aufweist. Ein solcher Datenträger ist beispielsweise aus der DE-OS 27 38 113 bekannt.

Die Erfindung wird nachfolgend anhand der Zeichnungen näher erläutert. Es zeigen:

Fig. 1 ein Datenaustauschsystem mit einer IC-Karte und einem Gerät;

Fig. 2 einen Authentisierungsablauf zwischen Karte und Gerät mit der Möglichkeit der Überprüfung des Geräts durch den Kartenbenutzer; und

Fig. 3 einen Authentisierungsablauf wie bei **Fig.** 2, bei dem Karte und Gerät unterschiedliche Schlüssel aufweisen.

Das Datenaustauschsystem gemäß der **Fig.** 1 besteht aus einer IC-Karte 1 sowie einem Gerät 3. Beide Systemkomponenten sind jeweils mit einer programmierbaren Steuereinrichtung versehen, die den in den nachfolgenden Figuren beschriebenen Funktionsablauf bewirkt. Ferner ist das Gerät 3 mit einer Anzeige 4 und einer Tastatur 5 versehen. Bei dem Gerät kann es sich um ein sogenanntes "off-line" betriebenes Terminal oder aber um ein "on-line"-Gerät handeln, das mit weiteren gleichrangigen Geräten einer Datenverarbeitungs-Zentrale verbunden ist.

In der **Fig.** 2 ist der chronologische Datenaustausch zwischen der Karte 1 und dem Gerät 3 zur Durchführung einer gegenseitigen Authentisierung, d. h. einer gegenseitigen Echtheitsüberprüfung, dargestellt. Ferner ist in diesem Ablauf vorgesehen, es dem Benutzer der Karte 1 zu ermöglichen, eine Überprüfung des von ihm benutzten Geräts im Hinblick auf seine Autorisierung vorzunehmen.

In der Karte 1 bzw. deren integriertem Schaltkreis 2 sowie in dem Gerät 3 ist jeweils eine Ver-/Entschlüsselungseinrichtung vorgesehen. In der Karte und dem Gerät ist jeweils ein zum Betrieb der Ver-/Entschlüsselungseinrichtung erforderlicher Schlüssel K vorgesehen. Dieser Schlüssel K ist in der hier beschriebenen Ausführungsform sowohl in der Karte als auch im Gerät vorgesehen, d. h. beide Systemkomponenten verfügen über den gleichen Schlüssel. Außerdem weisen sowohl die Karte als auch das Gerät jeweils einen bekannten Zufallszahlen-Generator und jeweils einen Vergleicher V1 bzw. V2 auf. In der Karte ist ferner ein vom rechtmäßigen Benutzer gewähltes Datenwort im Speicher des integrierten Schaltkreises 2 abgespeichert.

Mit Beginn der Authentisierung generiert das Gerät eine Zufallszahl R1, die von der Verschlüsselungseinrichtung unter Verwendung des Schlüssels K in eine Nachricht verschlüsselt wird. Diese Nachricht wird über eine Kommunikationsverbindung an die Karte übermittelt und von der Entschlüsselungseinrichtung der Karte unter Verwendung des Schlüssels K entschlüsselt. Das Ergebnis dieser Entschlüsselung ist die vom Gerät 3 generierte Zufallszahl R1.

Der Zufallszahlen-Generator der Karte generiert daraufhin eine Zufallszahl R2, die gleichzeitig mit der von der Karte ermittelten geräteseitigen Zufallszahl R1 sowie dem vom rechtmäßigen Benutzer der Karte gewählten Datenwort ROSE von der Verschlüsselungseinrichtung der Karte unter Verwendung des Schlüssels K zu einer Nachricht verschlüsselt an das Gerät 3 übermittelt wird. Im Gerät wird diese von der Karte übermittelte Nachricht der Entschlüsselungseinrichtung des Geräts zugeführt und unter Verwendung des Schlüssels K entschlüsselt. Als Ergebnis der Entschlüsselung liefert

die Entschlüsselungseinrichtung die geräteseitige Zufallszahl R1, das vom Benutzer gewählte Datenwort ROSE und die von dem IC der Karte generierte Zufallszahl R2. Die von dem Gerät entschlüsselte Zufallszahl R1, die aus der Nachricht der Karte stammt, wird dem Vergleicher V2 des Geräts zugeführt, der diese Zahl mit der Zahl R1 vergleicht, die von dem Gerät generiert und in verschlüsselter Form an die Karte gesandt wurde. Im positiven Falle geht das Gerät davon aus, daß es sich um eine zum Datenaustausch autorisierte Karte, d. h. eine echte Karte, handelt.

Nachfolgend wird der dechiffrierte Begriff ROSE der Karte auf der Anzeige 4 des Geräts 3 zur Anzeige gebracht. Dem Benutzer der Karte 1 an dem Gerät 3 ist damit die Möglichkeit eröffnet, zu überprüfen, ob die Anzeige 4 des Geräts 3 das von ihm gewählte Datenwort anzeigt, wodurch er sich versichern kann, daß es sich im positiven Fall um ein autorisiertes Gerät handelt, dem er im folgenden sein persönliches Merkmal, d. h. seine persönliche Identifizierungsnummer, preisgeben darf.

Damit auch kartenseitig die Echtheit des Geräts festgestellt werden kann, verschlüsselt die Verschlüsselungseinrichtung des Geräts die von dem Gerät entschlüsselte Zufallszahl R2 der Karte und sendet diese an die Karte. Die im IC-Schaltkreis 2 der Karte vorgesehene Entschlüsselungseinrichtung entschlüsselt diese Nachricht unter Verwendung des Schlüssels K, was die ermittelte Zufallszahl R2 liefert. Diese ermittelte Zufallszahl R2 wird mit der von der Karte generierten Zufallszahl R2 auf den in der Karte befindlichen Vergleicher R1 gegeben, der ein Vergleichsergebnis VE ausgibt, das binär codiert einem JA oder NEIN entspricht. Das Ergebnis dieses Vergleichs kann durch die Verschlüsselungseinrichtung der Karte unter erneuter Beteiligung des Schlüssels K verschlüsselt und an das Gerät übertragen werden. Dessen Entschlüsselungseinrichtung entschlüsselt die von der Karte 1 erhaltene Nachricht. Das Vergleichsergebnis VE zeigt dem Gerät, ob die Karte den Authentisierungsprozeß ordnungsgemäß durchgeführt hat.

Nachfolgend wird der Benutzer, wenn beide Vergleiche positiv verlaufen sind, von dem Datenaustauschsystem in bekannter Art und Weise zur Eingabe seiner persönlichen Identifizierungsnummer, d. h. seiner PIN, aufgefordert. Stimmt die vom Benutzer der Karte 1 eingegebene PIN mit der in dem System gespeicherten PIN, die dem rechtmäßigen Besitzer der Karte zugeordnet worden ist, überein, so erzeugt das Datenaustauschsystem eine Transaktionsfreigabe, die es dem Benutzer der Karte ermöglicht, seine Transaktionen, z. B. eine Geldüberweisung, vorzunehmen. Ebenso ist es denkbar, daß mit der Erzeugung der Transaktionsfreigabe dem Benutzer der Karte der Zugang zu einem überwachten Bereich ermöglicht wird.

Der in **Fig. 3** dargestellte Authentisierungsablauf zwischen der Karte 1 und dem Gerät 3 unterscheidet sich von dem Ablauf bezüglich der **Fig. 2** dahingehend, daß Karte und Gerät unterschiedliche Schlüssel aufweisen und daß das Gerät ferner einen gerätespezifischen Parameter, insbesondere eine gesonderte Zufallszahl, erzeugt. Das Datenaustauschsystem gemäß der **Fig. 3** verfügt, ebenso wie das Datenaustauschsystem gemäß der **Fig. 2**, über jeweils eine karten- bzw. geräteseitige Ver-/Entschlüsselungseinrichtung, separate Zufallsgeneratoren sowie separate Vergleichseinrichtungen.

In der Karte 1 ist ein Schlüssel KK sowie das vom rechtmäßigen Besitzer der Karte gewählte Datenwort ROSE in dessen integriertem Halbleiterschaltkreis 2 gespeichert. Ferner sind in diesem integrierten Schaltkreis die die Karte kennzeichnenden Daten, wie Bankleitzahl, Kontonummer des Karteninhabers usw., abgespeichert. Der nachfolgend verwendete Begriff "Kartendaten" beinhaltet einen Teil oder alle letztgenannten, benutzerspezifischen Daten sowie den Schlüssel KK und das Datenwort ROSE.

In dem Gerät 3 ist ein Geräteschlüssel KG sowie ein gerätespezifischer Parameter GID bzw. ein separater Zufallsgenerator, der den Parameter GID generiert, vorgesehen. Der Schlüssel der Karte KK ist über die Beziehung KK = EKG (Kartendaten) mit dem Geräteschlüssel KG verknüpft.

Der Authentisierungsablauf wird eingeleitet, indem die Karte die "Kartendaten" an das Gerät sendet. Im Gerät werden die Kartendaten mit dem Schlüssel KG verschlüsselt, womit das Gerät den Kartenschlüssel KK ermittelt. Der im Gerät befindliche Zufallsgenerator erzeugt daraufhin wie bei **Fig. 1** eine Zufallszahl R1, die mit einem gerätespezifischen Parameter GID unter Verwendung des Schlüssels KK verschlüsselt wird. Diese von der Verschlüsselungseinrichtung des Geräts verschlüsselte Nachricht wird an die Karte gesandt und entschlüsselt. Die Entschlüsselungseinrichtung der Karte liefert als Ergebnis die von dem Gerät 3 generierte Zufallszahl R1 sowie den gerätespezifischen Parameter GID.

Analog zu **Fig. 2** wird nun in der Karte 1 von deren Zufallsgenerator eine Zufallszahl R2 generiert, die mit der ermittelten Zufallszahl des Geräts R1 sowie dem von dem Benutzer gewählten Datenwort ROSE durch die Verschlüsselungseinrichtung der Karte unter Verwendung des gerätespezifischen Parameters GID als Schlüssel verschlüsselt wird. Diese Nachricht wird an das Gerät übermittelt und von der Entschlüsselungseinrichtung des Geräts wieder unter Verwendung des gerätespezifischen Parameters GID entschlüsselt. Als Ergebnis der Entschlüsselung liegen die ermittelte Zufallszahl R1 des Geräts, das Datenwort ROSE sowie die ermittelte Zufallszahl der Karte R2 vor. Der im Klartext vorliegende, vom rechtmäßigen Benutzer der Karte gewählte Begriff ROSE wird dem Benutzer der Karte in analoger Weise zu **Fig. 2** auf der Anzeige 4 des Geräts 3 angezeigt. Die vom Gerät generierte Zufallszahl R1 sowie die von dem Gerät ermittelte Zufallszahl R1 werden auf einen Vergleicher V2 in dem Gerät 3 gegeben. Im positiven Fall des Vergleichs geht das Gerät davon aus, daß es sich bei der verwendeten Karte um eine autorisierte Karte handelt.

Zur Feststellung der Echtheit des Geräts 3 durch die Karte 1 wird die von dem Gerät 3 ermittelte Zufallszahl R2 unter Verwendung des Kartenschlüssels KK von der Verschlüsselungseinrichtung des Geräts verschlüsselt. Diese Nachricht wird von dem Gerät 3 an die Karte 1 gesandt und dort von der Entschlüsselungseinrichtung der Karte unter Verwendung des Kartenschlüssels KK entschlüsselt. Als Ergebnis liegt die ermittelte Zufallszahl R2 vor, die von dem Vergleicher V1 im IC-Schaltkreis 2 der Karte 1 mit der von der Karte generierten Zufallszahl R2 auf Identität verglichen wird. Das Vergleichsergebnis VE wird unter Verwendung des Schlüssels KK in zur **Fig. 2** analoger Form verarbeitet.

Patentansprüche

1. Datenaustauschsystem, bei dem die Berechtigung eines Benutzers durch die Überprüfung eines

vom Benutzer eingegebenen persönlichen Merkmals festgestellt wird, mit einem dem Benutzer zugeordneten Datenträger, einer mit dem Datenträger kommunizierenden Vorrichtung und einer Anzeigeeinheit, **dadurch gekennzeichnet,** daß die Daten des Datenträgers ein nur dem Benutzer bekanntes Datenwort enthalten, das vor der Aufforderung zur Eingabe des persönlichen Merkmals zur Vorrichtung in codierter Form übertragen und nach der Decodierung durch eine in der Vorrichtung enthaltene und die Echtheit der Vorrichtung kennzeichnende kryptographische Einheit dem Benutzer zum Vergleich angezeigt wird.

2. Datenaustauschsystem nach Anspruch 1, dadurch gekennzeichnet, daß das Datenwort vom Benutzer bestimmbar und jederzeit änderbar ist.

3. Datenaustauschsystem nach Anspruch 2, dadurch gekennzeichnet, daß das Datenwort ein einprägsamer, für den Benutzer leicht zu merkender Begriff ist.

4. Datenaustauschsystem nach Anspruch 2, dadurch gekennzeichnet, daß eine Änderung des Datenwortes nur nach einem positiven Vergleich des eingegebenen persönlichen Merkmals mit einem im System gespeicherten Merkmal möglich ist.

5. Datenaustauschsystem nach Anspruch 1, dadurch gekennzeichnet, daß der Datenträger eine Ausweiskarte, Kreditkarte oder Zugangskarte ist, mit einem integrierten Schaltkreis mit Speicher- und Steuereinrichtung, daß das Datenwort in einem überschreibbaren Bereich des Speichers abgelegt ist und daß das Datenwort vor der Ausgabe an die Vorrichtung durch die Steuereinrichtung des integrierten Schaltkreises codiert bzw. verschlüsselt wird.

6. Datenaustauschsystem nach Anspruch 4, dadurch gekennzeichnet, daß die Steuereinrichtung ein programmgesteuerter Mikroprozessor ist.

7. Datenaustauschsystem nach Anspruch 4, dadurch gekennzeichnet, daß die Übertragung und Verschlüsselung des Datenwortes vom Datenträger zur Vorrichtung in einen zwischen dem Datenträger und der Vorrichtung ablaufenden Authentisierungsprozeß einbezogen wird.

8. Datenaustauschsystem nach Anspruch 6, gekennzeichnet durch einen Authentisierungsprozeß mit folgenden Schritten:

- die Vorrichtung generiert eine erste Zufallszahl (R1), die verschlüsselt an den Datenträger übertragen wird;
- der Datenträger entschlüsselt die empfangene Nachricht und bildet eine zweite Zufallszahl (R2);
- der Datenträger verschlüsselt die erste Zufallszahl (R1), das Datenwort und die zweite Zufallszahl (R2);
- die Vorrichtung entschlüsselt die empfangene Nachricht, vergleicht die entschlüsselte Zufallszahl mit der im Gerät erzeugten Zufallszahl und zeigt bei Übereinstimmung das entschlüsselte Datenwort auf einer Anzeigeeinheit an;
- die Vorrichtung sendet die verschlüsselte zweite Zufallszahl (R2) an die Karte;
- die Karte entschlüsselt die gesendete Nachricht und vergleicht die entschlüsselte zweite Zufallszahl mit der in der Karte erzeugten Zufallszahl und sendet bei positivem Vergleich eine Rückmeldung an die Vorrichtung;
- die Vorrichtung fordert den Benutzer zur Eingabe des persönlichen Merkmals auf.

9. Datenaustauschsystem nach Anspruch 7, dadurch gekennzeichnet, daß in die geräteseitige Verschlüsselung ein gerätespezifischer Parameter einbezogen wird.

10. Datenaustauschsystem nach Anspruch 8, dadurch gekennzeichnet, daß der gerätespezifische Parameter eine Zufallszahl ist.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 41 42 964 A1
Int. Cl.[5]: G 07 C 9/00
Offenlegungstag: 1. Juli 1993

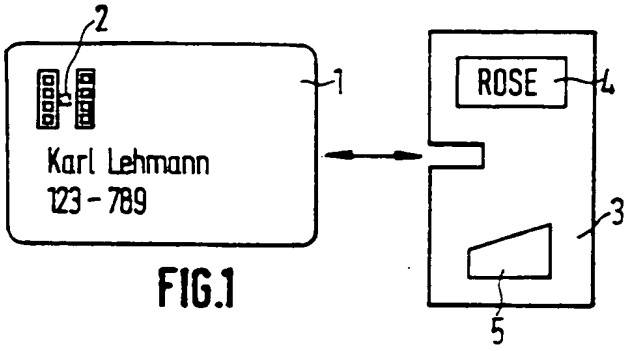

FIG.1

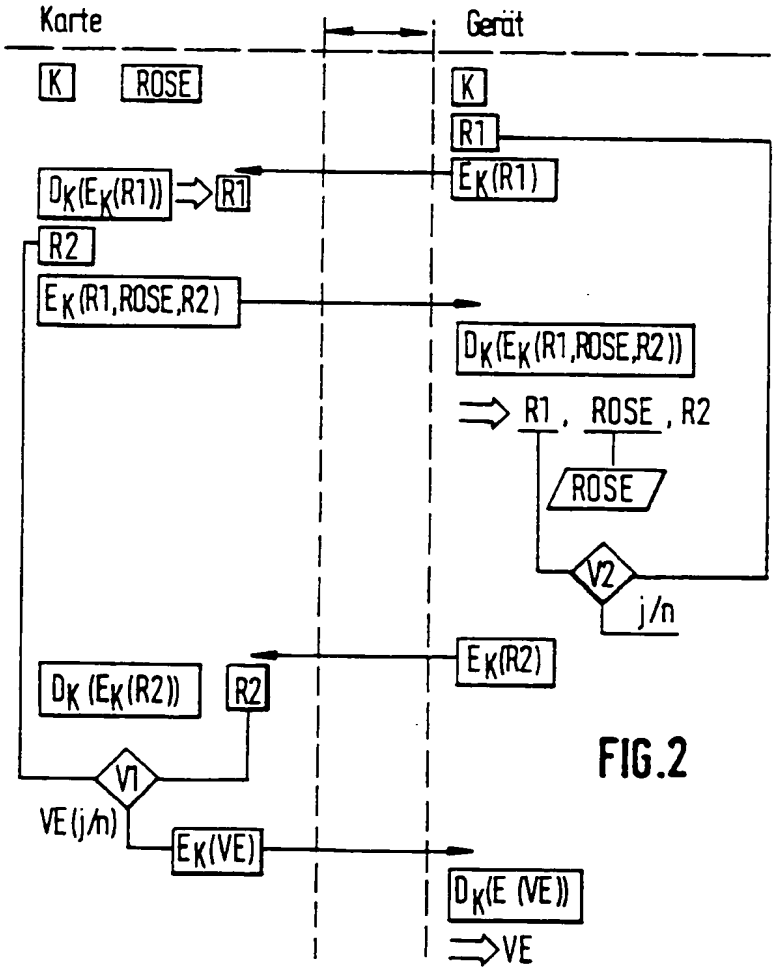

FIG.2

Nummer: DE 41 42 964 A1
Int. Cl.[5]: G 07 C 9/00
Offenlegungstag: 1. Juli 1993

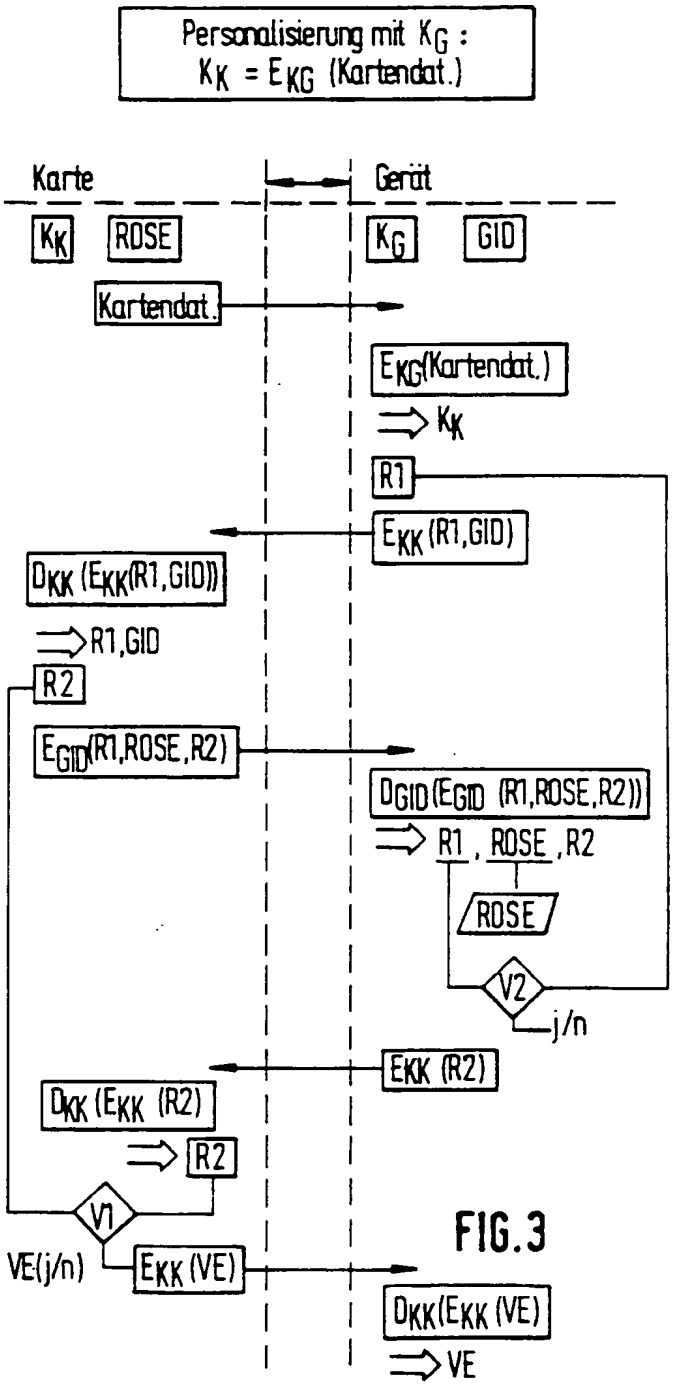

FIG.3